ARTÍCULOS

LEGISLACIÓN SOBRE COMPUTACIÓN EN LA NUBE Y NEGOCIACIÓN DE CONTRATOS

Charles Oppenheim

Charles Oppenheim fue profesor de ciencias de la información en la *Loughborough University* hasta su jubilación en 2009, y actualmente es profesor visitante en la *University of Queensland*. Ha ocupado varios puestos en el mundo académico y la industria editorial electrónica, trabajando para *International Thomson*, *Pergamon* y *Reuters* en varias ocasiones. Ha estado involucrado, dado conferencias, realizado servicios de consultoría, y publicado ampliamente sobre aspectos legales relacionados con la creación, difusión y consumo de la información -en especial los derechos de propiedad intelectual, licencias, protección de datos y libertad de información- desde mediados de la década de 1980. Es miembro de la *Junta Asesora Legal* de la *Comisión Europea*.

c.oppenheim@btinternet.com

Resumen

Se explican las características de los servicios de computación en la nube y se discuten las cláusulas que suelen incluir los contratos entre proveedores de dichos servicios y clientes. Mantener los datos en un servicio en la nube puede ser cómodo y más barato que en una instalación local de la propia organización, pero comporta varios riesgos. Se dan recomendaciones sobre cómo negociar los contratos, y se ofrece una lista de preguntas para obtener información del proveedor y así poder tomar una decisión bien informada que evite posteriores desagradables sorpresas.

Palabras clave

Computación en la nube, Contratos, Condiciones, Negociación, Características, Aspectos legales, Leyes, *Patriot Act*, Riesgos, Privacidad, Protección de datos, Derecho de autor, Copyright, Externalización, Recomendaciones.

Title: Cloud law and contract negotiation

Abstract

The main characteristics of cloud computing services are explained and the clauses typically included in contracts between suppliers and customers of such services are discussed. Keeping data on a cloud service can be more comfortable and cheaper than in a local installation of an organization, but it involves several risks. Recommendations are given on how to negotiate contracts. A list of questions to be asked to cloud service suppliers is provided, so a potential client can take an informed decision and to avoid unpleasant later surprises.

Keywords

Cloud computing, Contracts, Conditions, Negotiation, Features, Legal, Law, Patriot act, Risks, Privacy, Data protection, Copyright, Outsourcing, Recommendations, Relaciones proveedor-cliente.

Oppenheim, Charles. "Cloud law and contract negotiation". *El profesional de la información*, 2012, septiembre-octubre, v. 21, n. 5, pp. 453-457

http://dx.doi.org/10.3145/epi.2012.sep.02

Introducción

Los servicios de *cloud computing* o de computación en la nube proporcionan potencia de cálculo sin que el usuario tenga que tener hardware, software o contenido instalado en su lugar de trabajo local.

Wikipedia los define así:

"El *cloud computing* proporciona cálculo, software, acceso a datos y servicios de almacenamiento que no requieren que el usuario final sepa la localización física ni la configuración del sistema que ofrece los servicios.

La computación en la nube es un nuevo modelo de consumo y de ofrecer servicios de TI basados en protocolos de internet. Por lo general los recursos se pueden esca-

Nota: Este artículo puede leerse en su versión original inglesa en:
http://www.elprofesionaldelainformacion.com/contenidos/2012/septiembre/02_eng.pdf

Artículo recibido el 18-01-12

lar dinámicamente –ajustarlos a las necesidades de cada momento–, y a menudo virtualizarse. Es un subproducto y una consecuencia de la facilidad de acceso a sitios remotos de computación que proporciona internet. Puede tomar la forma de aplicaciones basadas en una web, a las que los usuarios pueden acceder y utilizar a través de un navegador como si los programas estuvieran instalados en su propia computadora local.

Es decir, los proveedores de *cloud computing* ofrecen programas a través de internet, a los cuales se accede desde un navegador web, y todo el software necesario y los datos de la empresa se almacenan en servidores ubicados en un lugar remoto. En algunos casos se trata de aplicaciones comerciales propietarias compartidas por varios usuarios, en otros, los programas son de diseño propio o a la medida.

La mayoría de las infraestructuras de *cloud computing* prestan servicios desde centros de datos compartidos con un único punto de acceso para las necesidades informáticas de los consumidores. Algunos clientes negocian las ofertas de los proveedores, obligándoles a cumplir acuerdos de nivel de servicio, pero eso es poco frecuente para el caso de las pymes".

Servicios como *Facebook*, *Rackspace*, *Hotmail*, *Twitter*, *Yahoo!*, *YouTube*, *Flickr*, *eBay*, *Google Apps* (y todas sus filiales, como *Gmail* y *Google Drive*), *Amazon EC2*, *TripAdvisor* o *DropBox* emplean u ofrecen servicios en la nube.

El interés por este modelo informático está creciendo, lo cual es muy comprensible, pues ofrece una forma barata y eficiente de *outsourcing* gestionando todo tipo de datos a las organizaciones que encuentran estas tareas gravosas, caras o que están más allá de su capacidad técnica.

Servicios en la nube y sus contratos

Los clientes de los servicios en la nube firman un contrato, que en la mayoría de casos no es negociable: o lo tomas o lo dejas. Sólo las organizaciones grandes o de prestigio tienen la influencia necesaria para exigir al proveedor que acepte enmiendas a los términos y condiciones estándar. Se han analizado varios contratos de servicios en la nube, y se ha demostrado que muchos de ellos son extremadamente unilaterales en favor del proveedor. Un ejemplo típico es el del servicio *iCloud* de *Apple*:

> "Usted reconoce y acepta que *Apple* pueda libremente acceder, utilizar, conservar y/o revelar la información de su cuenta y su contenido a las autoridades policiales, funcionarios del gobierno y/o un tercero, si *Apple* lo considera razonablemente necesario o apropiado, si se le requiere legalmente a hacerlo o si existe la creencia de buena fe de que tal acceso, uso, divulgación o conservación es razonablemente necesario para: (a) cumplir con procesos y requerimientos legales; (b) hacer cumplir este Acuerdo, incluyendo la investigación de cualquier posible violación del mismo; (c) detectar, prevenir o gestionar problemas de seguridad, fraude o técnicos; o (d) proteger los derechos, propiedad o seguridad de *Apple*, sus usuarios, terceros, o del público según requiera o permita la ley".

Si una persona u organización pequeña no está de acuerdo con los términos estándar que ofrecen, tiene que decidir entre correr el riesgo de aceptar el contrato estándar, probar con otro proveedor, o renunciar por completo a servicios en la nube.

Muy pocos contratos garantizan un buen servicio (por ejemplo, que funcione 100% del tiempo), y los que prometen reembolsos por cortes en el servicio o por escasa disponibilidad se caracterizan por reembolsar dinero de una futura renovación de la suscripción en lugar de un descuento en la suscripción existente. Así, si un cliente molesto por la poca disponibilidad decide no renovar o cancelar el contrato, no obtendrá ningún reembolso por los problemas sufridos. Algunos contratos dan al proveedor el derecho de cerrar el servicio sin previo aviso. Es de suponer que eso sólo lo haría si el servicio no le resultara rentable o si estuviera en serias dificultades financieras, pero el peligro es que el cliente que depende de él para sus actividades diarias puede quedar repentinamente en una situación difícil.

En general, los contratos tienden a incluir muchas obligaciones para los clientes y muy pocas para el proveedor de servicios. Pocos ofrecen encriptación automática de los datos que se les suministra y/o anonimización de datos personales. En los últimos años se ha hecho popular el concepto de evaluación del impacto de la privacidad (PIA), una evaluación independiente de los riesgos para la privacidad de un determinado servicio o sistema, junto con consejos sobre cómo solucionar las cosas si es necesario. Pocos contratos de nube incluyen referencias a los PIA. Asimismo, no permiten comprobar el cumplimiento de la privacidad a sus clientes.

Muchos proveedores de cloud incluyen una cláusula por la que se autoeximen de responsabilidad por los problemas que puedan surgir en el servicio, estén o no causados por su incompetencia o por imprudencia. La legalidad de este tipo de cláusulas no está clara, sobre todo cuando se impone a un individuo. Es realmente decepcionante que los proveedores de cloud incluyan este tipo de cláusulas, que indican inmadurez y falta de confianza en su negocio.

> "Algunos cláusulas de exención de responsabilidad de los proveedores de servicios en la nube indican inmadurez y falta de confianza en su industria"

La mayoría de empresas tienen algún tipo de información en sus sitios web sobre su política y sobre el procedimiento a seguir para pedir que se retire información (por ejemplo, que viole los derechos de autor o sea difamatoria). ¿Qué pasa si el sitio web lo mantiene un proveedor de servicios cloud? El contrato debería abordar la cuestión de la rapidez con que el proveedor de nube puede retirar materiales ofensivos si el cliente lo pide, pero la mayoría de los contratos no se ocupan de esta cuestión.

Los proveedores monitorizan el uso de ancho de banda y del hardware para realizar análisis estadísticos, planificar la actividad, etc., y de hecho algunas de estas estadísticas pueden ser útiles también para el cliente. Antes de firmar un contrato, éste debe examinar cuidadosamente los términos

del mismo para garantizar que se explican claramente los controles que se realizarán.

También debe describirse el procedimiento para eliminar datos cuando termine el contrato con el proveedor de servicios cloud. Probablemente el cliente deseará que todas las copias de los datos que obran en poder del proveedor de la nube se borren después de haber ejercido su derecho a que se le devuelvan. Y, por supuesto, tendrá que asegurarse de que los datos se le devuelven en un formato apropiado para un uso futuro de los mismos.

Protección de datos y seguridad en la nube

Casi por definición, los datos almacenados en la nube van a pasar de un país a otro, cada uno con sus propias leyes. Además el proveedor de servicios en la nube podría estar en un país diferente al de sus clientes. La situación se vuelve especialmente problemática cuando se considera la legalidad del contrato (por ejemplo, los diferentes requisitos de "imparcialidad" en diferentes países). En el caso de datos personales almacenados en la nube puede que haya que tener en cuenta las leyes de al menos 4 países: de la sede del proveedor de servicios, del cliente, del país del individuo cuya información se almacena, y las del país donde la nube pasa a residir físicamente en un momento dado. Pueden surgir problemas para determinar las responsabilidades, por ejemplo en el caso de que se filtren fraudulentamente datos personales. Y aunque no haya datos personales, pueden aplicarse las leyes de tres países (del proveedor de servicios, del cliente, y del país donde funciona la nube) a todas las operaciones realizadas con los datos o en posibles causas judiciales derivadas del contrato.

> "Los datos proporcionados a un proveedor de servicios en la nube pueden trasladarse de un país a otro sin que el cliente sepa cuándo ni dónde"

Numerosas encuestas de usuarios actuales y potenciales de servicios en la nube han puesto de manifiesto la preocupación existente por la seguridad de los datos, por ejemplo, que se pirateen, así como por la protección/privacidad, lo cual es un inhibidor potencial para su contratación. Los principales riesgos son la exposición de información confidencial y personal a los gobiernos, a los competidores, y a ladrones y oportunistas.

La naturaleza ubicua y dinámica de la nube significa que los datos facilitados a un proveedor de servicios en la nube se moverán de un país a otro sin que el cliente sepa cuándo ni dónde. Además los datos también pueden duplicarse y haber copias de seguridad en varios países. Igualmente es posible que varios proveedores cooperen, compartan los datos y los transfieran entre sus servidores. Sin embargo, las leyes de protección de datos (y otras) varían enormemente de un país a otro, y algunos no ofrecen ninguna protección real y práctica en su legislación. Lo ideal es que el contrato especifique quién es el responsable de mantener seguros los datos de carácter personal. Por otra parte, debería incluir también disposiciones para que el proveedor de servicios cloud indemnice a los particulares, o pague una posible multa si se infringe la legislación de protección de datos por culpa de un fallo suyo. Además, muchas leyes de protección de datos cuentan con un regulador oficial facultado para enviar notificaciones para que el titular de los datos haga algo, o para que suministre determinada información. El contrato debe asegurar que el servicio en la nube responda rápidamente a cualquier requerimiento.

En muchos países la legislación sobre protección de datos hace ilegal la transferencia de datos personales a un país sin leyes adecuadas de protección de los mismos a menos que la transferencia sea necesaria para un contrato concreto, cuente con la aprobación explícita de la persona, o existan razones especiales. La mayoría de los proveedores de servicios cloud son estadounidenses, aunque algunos tienen sede en filiales de la UE. Los que tienen sede en los EUA a menudo se comprometen a los "principios de puerto seguro", es decir, que los datos a su cargo sean instalados en un entorno físico en el que se respeten las leyes europeas de protección de datos. Pero no todos se comprometen a ello, y sería un servicio de nube muy raro si se comprometiera a no dejar salir los datos fuera del Espacio Económico Europeo. Los que no garantizan un puerto seguro representan por tanto un riesgo particularmente alto desde el punto de vista del cliente, ya que los datos podrían ir a un país con poca o ninguna consideración por las leyes de protección de datos. Es bastante preocupante que algunos de los mayores proveedores de servicios en la nube no se comprometan en sus contratos o bien a seguir las leyes europeas de protección de datos, o a colocar los datos del cliente en un puerto seguro. Por otra parte, los contratos no obligan a los proveedores a informar a un cliente si se ha expedido una orden de registro para inspeccionar los datos que almacena en el servicio.

Incluso si el proveedor se compromete a mantener los datos que se le encomiendan en un puerto seguro, ¿cómo se puede asegurar que siempre se quedarán ahí cuando la lógica de negocio de la nube es almacenar los contenidos en el lugar que sea más ventajoso económicamente? Los datos se guardarán en el primer centro de datos disponible y no pasará mucho tiempo para que sean trasladados a otro. Una aproximación a este problema potencial es conseguir que el proveedor de servicios en la nube acepte utilizar un puerto seguro combinado con la obligación contractual de "si algo sale mal el proveedor estará sujeto a las reglas de la ley de protección de datos de la UE". Entonces, si algo fuera mal, el proveedor sería penalizado como si estuviera operando en la UE. Pero como se señaló anteriormente, los proveedores de servicios cloud son notoriamente reacios a negociar los términos contractuales. No obstante, se recomienda encarecidamente que el cliente potencial exija que se apliquen esos principios básicos del puerto seguro.

Patriot act

Un área de preocupación particular es la ley *Uniting and strengthening America by providing appropriate tools required to intercept and obstruct terrorism* (Unir y fortalecer América mediante los instrumentos adecuados necesarios para interceptar y contrarrestar el terrorismo), más conocida como *Patriot act*. Esta ley de gran alcance permite a las

autoridades estadounidenses obligar a los proveedores de servicios de internet (ISP) y a los proveedores de servicios cloud, entre otros, a dar información sobre sus clientes y/o los datos que almacena o utiliza, sin que éstos sepan que tal información ha sido solicitada. A pesar del título de la *Ley*, su uso puede extenderse más allá del terrorismo a otros tipos de investigación criminal. Debido a sus amplios poderes, esta *Ley* ha sido vista con desagrado por los países que cuentan con una legislación bien desarrollada de protección de datos, y ha llevado a algunos gobiernos (por ejemplo, Canadá y Holanda) a prohibir a sus organizaciones nacionales que pasen datos a organizaciones de los EUA. Según parece *Amazon* retrasó el lanzamiento de su nuevo *Kindle Fire* en la UE por la incompatibilidad de la *Patriot act* con la legislación comunitaria sobre protección de datos.

La cuestión clave para un cliente de cloud, por tanto, no es sólo si el servicio ofrece un puerto seguro para su información, sino también si quiere correr el riesgo de que sus datos puedan terminar en manos de las autoridades de Estados Unidos, como resultado de la *Patriot act*. Hay que informarse y analizar todo eso, y lo recomiendo si los datos son especialmente sensibles, ya sean personales, o comerciales confidenciales. Es uno de los muchos factores de riesgo que hay que tener en cuenta al contratar un proveedor de servicios cloud. La *Ley Patriot* no es única, por supuesto, hay legislaciones similares en otros países donde pueden instalarse los datos, pero no suelen tener tanto alcance o no son tan conocidas como la *Patriot*.

Seguridad

Las cuestiones de seguridad son también una preocupación importante. Ha habido casos anecdóticos en los que por períodos de tiempo cortos un cliente de un servicio de nube podía leer los materiales de otro. Un cliente potencial, por tanto, debe realizar las diligencias apropiadas sobre el servicio que piensa utilizar y cerciorarse de que la seguridad está en el nivel apropiado para el valor y/o la sensibilidad de la información. Es aconsejable probar el servicio en la nube por primera vez con información no confidencial. Recomiendo que se negocie para que el contrato incluya una cláusula que obligue al servicio a cumplir ciertas normas específicas de seguridad internacionales, y/o las normas de seguridad propias del cliente. El contrato debe explicitar la responsabilidad (y sus límites) del proveedor de servicios en caso de pérdida de datos o de un fallo de seguridad. Los clientes deben negarse a firmar un contrato que exima al servicio de la nube de toda responsabilidad por pérdida de datos o violación de la seguridad.

Otras cuestiones jurídicas

Protección y seguridad de los datos no son los únicos problemas legales que pueden surgir. También podrían aparecer otros sobre quién es responsable si alguien modifica los datos ofrecidos por un cliente y su liberación resulta ser ilegal, como una difamación o una infracción de las leyes de seguridad nacional. No está claro en estos casos de qué país podrían aplicarse las leyes. Si bien es poco realista esperar que el proveedor de servicios en la nube controle todo en sus servidores (y de hecho, esto podría ser problemático desde el punto de vista de la privacidad), es razonable esperar que responda a las quejas recibidas sobre presuntos comentarios difamatorios. El contrato o un acuerdo de nivel de servicio adicional entre el cliente y el proveedor de servicios cloud probablemente incluirá las garantías y las instrucciones relativas a las supuestas declaraciones difamatorias u otros materiales potencialmente ilegales almacenados en los servidores.

Las licencias de software, de derechos de autor y de bases de datos también son -hasta cierto punto de forma sorprendente-, potencialmente problemáticas. Si un cliente tiene permiso para utilizar un software o base de datos "in situ", ¿incluye eso "en la nube"? Una licencia puede establecer que el material no debe ser enviado a otro país. Las restricciones pueden incluso ir más allá, declarando que una base de datos o software sólo se podrá utilizar en un único equipo, o sólo por los empleados de la institución. Si dichas bases de datos y/o software van a ser colocados en la nube, las licencias tendrán que ser renegociadas. Muchos propietarios de bases de datos y de licencias de software son conscientes de la existencia de la nube y están dispuestos a ser flexibles en esta materia. Si no lo son habrá que tomar una decisión sobre si colocar ese producto en la nube, o utilizar uno alternativo que no imponga ninguna restricción.

Por último, los clientes deben asegurarse de que el contrato confirma que la propiedad de los derechos de autor y otros derechos de propiedad intelectual de los materiales mantenidos en la nube sigue siendo de los propietarios originales, y no se transfieren al servicio de nube.

Preguntas que se deben hacer antes de firmar

A continuación se presenta una lista de preguntas a formular a los proveedores de servicios en la nube antes de firmar un contrato:

- ¿Quién será capaz de ver mi información? (tanto dentro como fuera del proveedor de servicios).
- ¿Quién posee y controla su infraestructura? ¿Está subcontratada a terceros?
- ¿Dónde se encuentran las instalaciones? (a continuación, comprobar cuáles son las leyes de protección de datos de esos países, y si la respuesta es "no se sabe en qué países podrían almacenarse los datos", es mejor no firmar con ese proveedor).
- ¿Puedo ver una copia de sus informes sobre fiabilidad, disponibilidad y tiempo de inactividad (si los hay)?
- ¿Qué niveles de servicio garantizan, por ejemplo, disponibilidad, tiempo necesario para resolver un problema, y qué compensación ofrecen si no cumplen eso? (en particular, los posibles clientes deben oponerse a la práctica estándar actual de descuentos en las suscripciones futuras, e insistir en que sea posible recibir una compensación económica en el acto, y/o poder terminar el contrato anticipadamente con derecho a reembolsos).
- ¿Han tenido fallos de seguridad en el pasado? (si responde "sí", pregunte más detalles).
- ¿Tendré un nombre de contacto dentro de la organización en caso de algún problema?
- ¿Cumplirán nuestra *Ley de Protección de Datos* (si aplica) al manejar mi información? ¿Van a pagarme daños y perjuicios si ocurre una violación de la ley por culpa suya?

¿Qué garantías puede dar de que se cumplan las leyes de protección de datos incluso si los datos que suministramos se almacenan en un país con una débil o ninguna ley de protección de datos, o cuando los poderes de inspección del gobierno sean de muy gran alcance?
- ¿Sería fácil migrar mis datos a un servicio competidor una vez haya terminado este contrato? ¿Pueden garantizarme que me los devolverán en un formato utilizable?
- ¿Quién es el responsable de la gestión de passwords y control de acceso en su empresa?
- ¿Cuáles son los nombres de los empleados encargados de manejar los datos?
- ¿Qué políticas de seguridad, tecnología y sistemas emplean? ¿Qué normas nacionales o internacionales cumplen?
- ¿Tengo derecho a negarme antes de que realicen cambios en el servicio que afecte a mis datos? (también: si no estamos de acuerdo con determinados cambios en los servicios, ¿podemos cancelar el contrato anticipadamente y obtener una compensación económica?).
- ¿Van a utilizar el nombre de mi organización o el tipo de nuestros datos en su publicidad? (si es el caso, exigir que el proveedor pida permiso cada vez).
- ¿Qué medidas especiales tomarán con los datos que etiquetemos como confidenciales?
- ¿Podríamos hacer una prueba con algunos datos no sensibles antes de comprometernos?
- ¿Están dispuestos a incluir cláusulas en el contrato asegurando que no va a haber pérdida o destrucción no autorizada de los datos?
- ¿Pueden darnos periódicamente copias de seguridad de todos nuestros datos?
- ¿Se comprometen a informarnos si tienen conocimiento de alguna violación de la seguridad de datos que afecte o involucre a nuestros datos?
- Por último, y lo más importante, ¿es su contrato negociable?

Algunas de estas preguntas pueden ser contestadas en el borrador de contrato, en los documentos publicados por el servicio o en conversaciones informales con los ejecutivos de ventas. Sin embargo, se debe presionar para que algunas de las respuestas figuren en el propio contrato o en un acuerdo de nivel de servicio adicional, es decir, no debemos contentarnos con promesas informales. El verdadero problema en el uso de servicios en la nube es que los clientes entran en una relación de términos y condiciones con poco poder para negociar. Para sentirnos cómodos hay que confiar en el proveedor y serán las respuestas a las preguntas anteriores (o la negativa a darlas) las que justificarán (o no) esa fe.

Como conclusión: uno no debe volverse paranoico con la nube, pues ofrece muchos beneficios potenciales, pero debemos firmar los contratos siendo conscientes de los beneficios y de los riesgos, y debemos hacer una evaluación informada de los riesgos antes de comprometernos.

Algunos recursos y bibliografía reciente

Carlton, Gregory H.; **Zhou, Hill**. "A survey of cloud computing challenges from a digital forensics perspective". *Intl Journal of Interdisciplinary Telecommunications and Networking*, 2011, v. 3, n. 4, pp. 1-16.
http://dx.doi.org/10.4018/jitn.2011100101

Cheng, Fa-Chang; **Lai, Wen-Hsing**. "The impact of cloud computing technology on legal infrastructure within internet-Focusing on the protection of information privacy". *Intl workshop on information and electronics engineering, Procedia engineering*, 2012, v. 29, 2012, pp. 241-251.
http://dx.doi.org/10.1016/j.proeng.2011.12.701

González, Nelson; **Miers, Charles**; **Redigolo, Fernando F.**; **Carvalho, Teresa C.**; **Simplicio, Marcos A.**; **Naslund, Mats**; **Pourzandi, Makan**. "A quantitative analysis of current security concerns and solutions for cloud computing". En: *IEEE 3rd intl conf on cloud computing technology and science (CloudCom)*, Nov. 29 2011-Dec. 1 2011, pp. 231-238.
http://dx.doi.org/10.1109/CloudCom.2011.39

Hay, Brian; **Nance, Kara**; **Bishop, Matt**. "Storm clouds rising: security challenges for iaas cloud computing". En: *44th Hawaii intl conf on system sciences (Hicss)*, 4-7 Jan. 201, pp. 1-7.
http://dx.doi.org/10.1109/HICSS.2011.386

Inteco-Cert. *Riesgos y amenazas del cloud computing*. Madrid: Instituto Nacional de Tecnologías de la Comunicación; Mº de Industria, Turismo y Comercio; Plan Avanza 2; marzo 2011, 32 pp., 489 KB
http://cert.inteco.es/extfrontinteco/img/File/intecocert/EstudiosInformes/cert_inf_riesgos_y_amenazas_en_cloud_computing.pdf

Klein, Carolina A. "Cloudy confidentiality: clinical and legal implications of cloud computing in health care". *J Am Acad Psychiatry Law*, 2011, v. 39, pp. 571–578.
http://www.jaapl.org/content/39/4/571.full.pdf+html

Legal Cloud Computing Association
http://www.legalcloudcomputingassociation.org

Mell, Peter; **Grance, Timothy**. *The NIST Definition of Cloud Computing. Special Publication 800-145*. Computer Security Division, Information Technology Lab., National Institute of Standards and Technology, Gaithersburg, MD 20899-8930, Sept. 2011, 7 pp.
http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf

National Archives of Australia. *Records management and the cloud - a checklist*, 2011, 5 pp., 444 KB
http://www.naa.gov.au/Images/Cloud_checklist_with_logo_and_cc_licence_tcm16-44279.pdf

Schweitzer, Eugene J. "Reconciliation of the cloud computing model with US federal electronic health record regulations". *J Am Med Inform Assoc*, 2012, v. 19, pp. 161-165.
http://dx.doi.org/10.1136/amiajnl-2011-000162
http://jamia.bmjjournals.com/content/19/2/161.full.pdf+html

Wood, Katie; **Anderson, Mark**. "Understanding the complexity surrounding multitenancy in cloud computing". En: *IEEE 8th Intl Conf. on e-Business Engineering (Icebe)*, 19-21 Oct. 2011, pp. 119-124.
http://dx.doi.org/10.1109/ICEBE.2011.68